



[Blog Posts](#)   [About us](#)   [How our blog works](#)   [Writing for RHUL Geopolitics](#)

# Cyber War, Supply Chains, and Realism in Lithuania

RHULGeopolitics / July 17, 2019



Vilnius Summer School attendees (source: [Vilnius Summer School](#))

For national security actors in Lithuania, Russia is a vital aspect of most conversations. In July 2019, co-editor Nick Robinson and myself attended [a week-long cyber security course](#) in Lithuania's capital Vilnius. The event was organised by former serviceman Dr Erikas Kaukas, and energy security advisor Ms Jurgita Jakevičiūtė. Entitled 'Digital Warfare on the Eastern front', there could be no mistake that Russian cyber-operations would be the dominant topic of discussion.

## A Story of Resistance

There was a recurring narrative we found when we spoke to politicians, NATO officers, cyber security experts, and even tour guides: Lithuania will **not** be occupied again.

Lithuanians understand themselves as an ancient people, who retained their pagan connection to the natural world by uniting together as a kingdom against crusading Teutonic Knights. It is important to understand Lithuanian history from the origins of the nation itself. The common narrative of Lithuania is that of a nation forged in the common defence of their homeland from foreign invasion. Over the centuries, Lithuania secured allies, and expanded to lands which now cover contemporary Estonia, Latvia, and Poland, and also formed a notable commonwealth of Poland and Lithuania, before being consumed by the Tsarist Russian empire of the 19th century. The nation came back into independent existence in the inter-war period, only to alternate between Soviet (1940-1941 and 1944-1991) and Nazi (1941-1944) control in the latter half of the 20th century, and eventually re-secured independence in the 1990's. In 2004, Lithuania joined both the European Union and NATO, signalling geopolitical alignment to 'the West'.

Today, Lithuania finds itself in a vulnerable situation: Russia (and its ally Belarus) looms in the East, and squeezes Lithuania to the west with the Kaliningrad enclave (Fig.1). Authorities we spoke with emphasised that events in [Georgia](#), [Estonia](#), [Ukraine](#), and more specifically [Crimea](#), give good cause for Lithuania to be highly suspicious of Russia's presence on both sides of their state. After the Crimean annexation of 2014, [NATO re-vamped their commitment to Lithuanian sovereignty](#). The recurring narrative of 'resisting domination' manifests itself in a strategy of multifaceted national security, and one of the most interesting aspects have been tactics utilised in the cyber domain.



Fig 1. Russian enclave to the West of Lithuania, Belarus South-East, and Russia looming in the East ([Source](#))

## Realism About Russia

In geopolitics, 'realism' is a term that considers conflict to be an unavoidable fact of the world. As an ideology, it contains Darwinist elements of competition being 'natural', Machiavelli's shrewdness of how one should view one's enemies (summary: with great suspicion, and a plan for their demise), and Hobbesian elements of a population submitting their support to the sovereign who offers in return their safety and security. Realist scholars (which include the geographer [Halford Mackinder](#)) reference Thucydides, and his account of the 431 BC Peloponnesian War, to argue the patterns and behaviours of 'inevitable conflict' from the ancient world can be transposed and learnt from in the modern world. To realists, the Roman maxim resonates: *'If you want peace, prepare for war'*.

However one feels about realism as a concept, it is safe to say that realism towards Russia informs the political-military doctrine of Lithuania. During our visit, officials thematically communicated their realist doctrine through their narrative of national resistance against various oppressors. This script of resistance is a key aspect of Lithuania's [ontological security](#), whereby particular actions and phrases become routine when their objective is to achieve feelings of self-security. Conflict with Russia is seen as an inevitable fact of Lithuania's present and future existence, and their continuous efforts to secure cyberspace from daily cyberattacks and disinformation emanating from Russia provides regular vindication for their suspicions.

## Digital War in Lithuania



Fig 2. Insignia for cyber security arm of the Ministry of National Defence ([source](#))

Lithuania is well-versed in combatting tactics from the Russian cyber-operation playbook. In terms of defending against malicious Russian malware, one official pointed to the lengths they went to in order [to secure the elections earlier](#) this year; creating their own secure (operating) software to use on computers that were collecting votes. On the other hand, disinformation is an arduous cyber operation to defend against, as Russia had proven adept at fabricating news stories such as [a Lithuanian child being raped by NATO soldiers](#). An official described the objective of Russian information warfare as "breaking minds", and recognised that this was something incredibly difficult to defend against. One defensive tactic the government has taken has been to forge closer relationships with news media outlets in Lithuania, thereby making it easier to verify sources and stories, as well as pull fake news stories off of websites quicker.

Russian digital interference takes many paths, including the digital supply chain. Concerns regarding the digital supply chain have reached contemporary notoriety, as might be seen in the recent controversy surrounding [Huawei products](#). Russian-based companies who manufacture routers have been scrutinised for the hardware they produce, and [the potential for cyber espionage](#). Hardware is not the only route interference may take. Software produced by Yandex (the Russian equivalent of Google) has also been treated with suspicion. Yandex has also produced an Uber-like cab-hailing app, which is extremely cheap to use in comparison to competitors. We were told that the Lithuanian state has examined the app, and found [that it extracts data from a user's phone](#) without them knowing, and travels through a myriad of different countries, but ultimately implicates actors in Russian territory. Now, this is all *alleged*. But Lithuanian security actors are taking no risks.

## Digital Defence

We received an education on the tactics the Ministry of National Defence has deployed in order to thwart Russian interference against critical national infrastructure. To me, this is where Lithuania provides a truly fascinating case study. We arrived at the Lithuanian government cyber security centre on a rainy Monday, and were politely asked to leave our phones at the entrance. It would be unwise for me to go into immense detail of what exactly we saw, but in essence this cyber department was designing, manufacturing, and distributing its own hardware for government networks and critical national infrastructure. Lithuania did not trust certain global supply chains that may have links back to either Russia or China, and so this department developed their own hardware (fig 3).

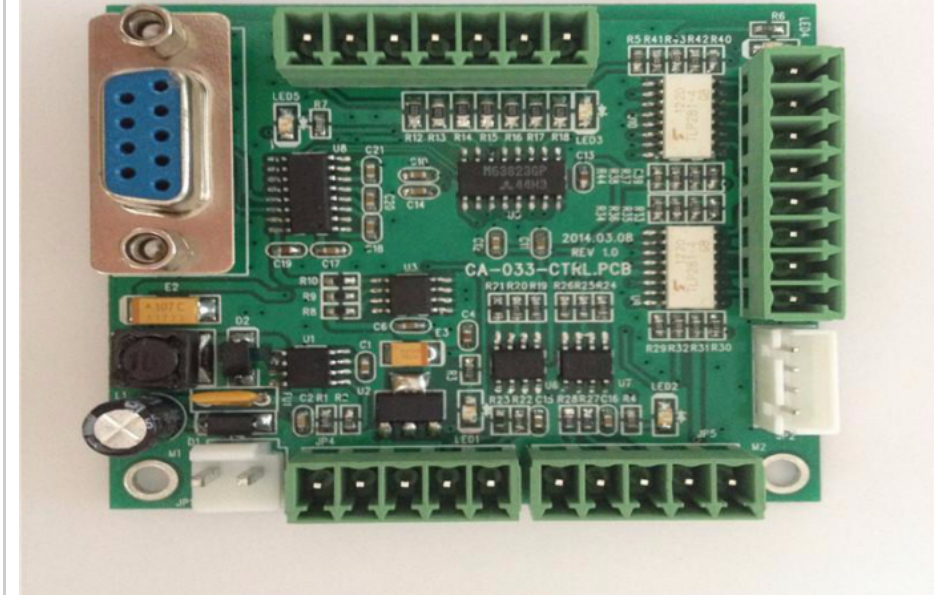


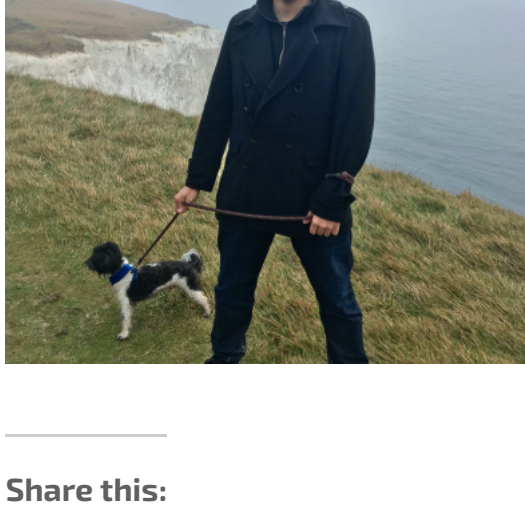
Fig 3. An example of a hardware chipboard, similar to the one used in our demonstration ([source](#))

Each room was a node in the production line that produced the hardware. We were able to see where the designers think of what they want the motherboard to be capable of, how they sketch this on their computers, and then where their visions are realised and assembled. To truly emphasise how serious Lithuania was about securing its own supply chains, we were invited to try and solder pieces of the motherboard together and experience for ourselves how difficult, but worthwhile this was, in order to be able to trust one's own equipment. In their fight against Russian interference, Lithuanian realist suspicions are exemplified by this desire to produce their own hardware.

## The Future of Cyber Supply Chains

Throughout our trip, it became clear that alliances such NATO and the EU were key parts of the Lithuanian narrative to never be occupied again. An official told us of his vision to form better unity within these alliances, and especially develop [EU cyber defences](#) to be more communicative and coherent. One of his ambitions was for Lithuania to be the trusted supplier of hardware to other allies in Europe and America. He also expressed hope for cyber security experts to come to Lithuania and take part in training, exercises, and information sharing to foster better cooperation across borders.

The cyber component of Lithuanian national security was just one aspect of their nuanced defences. Cyber security sits under the Lithuanian Ministry of National Defence, and it was demonstrated to us that Lithuania sees cyber as one tool in an arsenal of many to protect itself from their enemy. The geopolitics of the situation in Lithuania is fascinating, and I will be following the nation's cyber strategy closely moving forward.



[Dray Agha](#) is an EPSRC-funded PhD student at RHUL. He keenly reads up all things cyber, ideas of State power, and how to action a peaceful, cooperative future. You can find him on Twitter [@DrayBafA](#).

Share this:

[Twitter](#)   [Facebook](#)   [Tumblr](#)   [LinkedIn](#)

[Like](#)

One blogger likes this.

July 17, 2019 in VISIT.

## Related posts

**NEWS | RHUL Geopolitics and CDT in Cyber Security continue to flourish in partnership**

**Of Other Cyber Securities: workshop next week at RHUL**

**NEWS | Curating (in)security at AAG 2017**

[← Independent Oversight of Detention Facilities – Why Does it Matter?](#)

[‘Evacuated to Death’ paper is out. Some ‘Political Atmospherics’ too. →](#)

## Leave a Reply

Enter your comment here...

## Follow us on Twitter

Tweets by [@RHULGeopolitics](#)

**Reclaiming Success** [@ReclaimingSucc](#)  
This week's instalment of [#ReclaimingSuccess](#) is from the wonderful [@olivia\\_r\\_mason](#): [#7 - You will overcome this!](#) [reclaimsuccess.wordpress.com/2020/03/06/7-y...](#)

Mar 6, 2020

**MasterGeomatiqueUnivCerg** [@MGeomatique](#)  
Let's go 🇵🇧  
[#workshop@RHULGeopolitics](#)  
[@UniversiteCergy](#)

Feb 21, 2020

**MasterGeomatiqueUnivCerg** [@MGeomatique](#)  
Day 4 of our Workshop ! Every team is working harder than ever, the final presentation is tomorrow 🙌🏻  
[#workshop](#) [#CY@RHULGeopolitics](#)  
[@UniversiteCergy](#)

Feb 20, 2020

**Julien Lecaché** [@JLecache](#)  
Today was a very productive day, it was the beginning of the map creation and the finalization of the data collection. The scenario for securing a protest is moving forward! [#gis](#) [#workshop](#)  
[@RHULGeopolitics](#) [@MGeomatique](#)



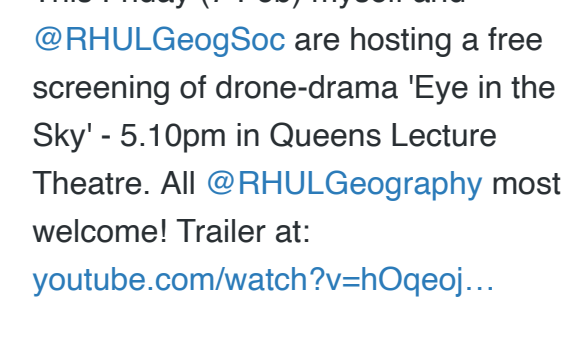
Feb 19, 2020

**MasterGeomatiqueUnivCerg** [@MGeomatique](#)  
Our three groups working with our colleagues from the Royal Holloway. Cooperation is key!  
[@UniversiteCergy](#)  
[@RHULGeopolitics](#) [#workshop](#) [#CY](#) [#GIS](#)



Feb 18, 2020

**Dr. Anna Jackman** [@ahjackman](#)  
Free film screening 🎬  
This Friday (7 Feb) myself and [@RHULGeogSoc](#) are hosting a free screening of drone-drama 'Eye in the Sky' - 5.10pm in Queens Lecture Theatre. All [@RHULGeography](#) most welcome! Trailer at: [youtube.com/watch?v=hOqej...](#)



Feb 3, 2020

**Dr. Anna Jackman** [@ahjackman](#)  
Thanks so much for the invite, [@katehallgeog](#) 🙌 Really looking forward to chatting drones!  
[https://twitter.com/katehallgeog/status/1192718608625029120](#)

Nov 8, 2019

[Embed](#)   [View on Twitter](#)

Search ...